STRATEGY RESEARCH PROJECT

IMPLEMENTATION OF INFORMATION SANCTIONS

BY

LIEUTENANT COLONEL GEORGE S. BROCK
United States Marine Corps

USAWC CLASS OF 1997

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

IMPLEMENTATION OF INFORMATION SANCTIONS

by

LtCol George S. Brock

Captain R. L. Recordon, USNR
Project Advisor

U. S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: George S. Brock (LtCol), USMC

TITLE: Implementation of Information Sanctions

FORMAT: Strategy Research Project

DATE: 14 April 1997 PAGES: 31 CLASSIFICATION: Unclassified

The expansion of information technologies and the close correlation between access to these technologies and the economic welfare of nations highlights an emerging dimension through which economic materials could be interdicted. There is little historical precedence to analyze the effectiveness of such sanctions during the deterrence (pre-conflict) phase of a crisis. The process of enacting and enforcing information sanctions targeted at a Nation's strategic information systems has not been refined. In order to analyze the process through which information sanctions could be enacted and enforced, a review of past sanctions enforcement operations will provide a foundation for the process. With this foundation, the evolution of information systems and their growing association with a global economy will be reviewed to provide insights into the potential effectiveness of information sanctions. The process of enacting information sanctions, choosing information system targets, and deciding upon which agency is most capable of enforcing information sanctions will be hypothesized.

TABLE OF CONTENTS

Information sanctions should be considered as potentially effective instruments of national power when employed during the early stages of a crisis in order to deter conflict. Should deterrent measures fail, information sanctions enacted during the deterrent phase of the evolving crisis could serve as the foundation for follow-on information operations.

The United States' National Military Strategy (NMS) identifies the act of sanctions enforcement as an instrument of our national power that may be employed in order to deter conflict. The NMS specifies the role of military forces with respect to sanctions enforcement operations as follows:

> Military forces are increasingly used to enforce economic sanctions resulting from national policy decisions and UN Security Council resolutions. US Forces will participate in operations to search, divert, delay or disrupt transport vessels and to assist in the compliance of guidelines set by either US or UN authorities.[1]

Examples of military operations to enforce sanctions are numerous however, such operations have focused upon the physical interception of specified materials and not targeted information for interdiction.

The Department of Defense has recognized the growing importance of information as a commodity within the context of global affairs and published Joint Chief of Staff Memorandum of Policy (MOP) 30 in 1993. MOP 30 defines the new facet of information warfare (IW) as having "... five essential elements, sometimes called the 'five pillars': deception, operational security (OPSEC), electronic warfare (EW),

psychological warfare (PSYOP), and physical destruction."[2] Command and control warfare (C2W) is defined as the strategy that implements the military elements of IW. Military efforts within the IW field have focused upon targeting enemy military command and control nodes and not addressed a role in enforcing strategic level information sanctions against a target nation.[3]

The expansion of information technologies and the close correlation between access to these technologies and the economic welfare of nations highlights an emerging dimension through which economic materials could be interdicted. There is little historical precedence to analyze the effectiveness of such sanctions during the deterrence (pre-conflict) phase of a crisis. The process of enacting and enforcing information sanctions targeted at a Nation's strategic information systems has not been refined.

In order to analyze the process through which information sanctions could be enacted and enforced, a review of past sanctions enforcement operations will provide a foundation for the process. With this foundation, the evolution of information systems and their growing association with a global economy will be reviewed to provide insights into the potential effectiveness of information sanctions. The process to enacting information sanctions, choosing information system targets, and deciding upon which agency is most capable of enforcing information sanctions will be hypothesized.

SANCTIONS ENFORCEMENT OPERATIONS

Prior to the end of the cold war, there was little chance of enacting sanctions through the United Nations due to Soviet and United States veto authority within the security council. Of the 116 economic sanctions initiated between World War I and 1990, 78 were initiated by the United States. The majority of these 78 sanctions were unilateral in nature and the remainder included voluntary support from close allies.[4] The only two sanctions issued by the Security Council prior to 1990 were anti-apartheid sanctions leveled against Rhodesia, and South Africa. This dominance of unilateral actions was reversed with the end of the cold war. Since 1990, the Security Council has issued sanctions against Iraq, former Yugoslavia, Somalia, Libya, Haiti, Liberia, and the UNITA rebels in Angola.[5] The following paragraphs provide an overview of two cases in which sanctions were implemented; prewar Iraq, and former Yugoslavia.

Prewar sanctions against Iraq were imposed quickly with full international support. Economic sanctions were in place within one week of the Iraqi invasion of Kuwait, approval of the use of naval forces to enforce the sanctions followed within a month, a month later sanctions were expanded to include an air embargo and a secondary boycott of countries violating the resolutions.[6] The U. S. led plan to implement and enforce the sanctions was comprehensive and included coordination with other mideast oil producing states to increase production and offset the loss of oil produced in Iraq and Kuwait. The plan also included an "economic action" plan to aid countries whose

economies were most severely impacted by the inevitable rise in oil prices.[7] Sanctions enforcement was simplified due to the lack of diversity of the Iraqi economy (90 percent of export revenue came from oil), and the geographic isolation of the country.[8] Although these prewar sanctions were strongly enforced, they failed to remove Iraqi forces from Kuwait.

In contrast to the swift and comprehensive sanctions enforced in response to the Iraqi invasion of Kuwait, the Security Council was not able to pass comprehensive economic sanctions against the former Yugoslavia until one year after initial fighting began. The authorization for naval forces to enforce the sanctions was not passed until five months later. The sanctions did not include the imposition of secondary sanctions against countries violating the resolution or any type of compensation plan. Six months after the passage of the original Security Council resolution, the passage of another resolution was required in order to prevent Serbian misappropriation of transshipment goods. The failure to implement a comprehensive sanction enforcement plan coupled with the complex geography and diverse economy of the country complicated sanction enforcement efforts.[9]

The salient trends which appear when post cold war sanctions and associated enforcement operations are reviewed include a growing propensity for the United States to lead the initiation of United Nations resolutions which impose sanctions upon nations in order to achieve our national objectives. The review highlights that sanctions must be imposed quickly, decisively, and supported by a broad coalition in order to be potentially

effective. The construct of the U. N. resolutions which authorize the sanctions must mandate measures to facilitate enforcement such as secondary sanctions which punish nations which violate the resolutions, and provisions for monitoring of sanctions compliance by independent agencies. Coalition military forces required to support sanction enforcement operations must be identified and sourced. A comprehensive sanctions resolution must also make provisions to economically compensate countries suffering second order effects from sanction implementation, and include plans to provide humanitarian aid to the general populace of the target country.[10]

In the Iraqi example, even when sanctions were imposed comprehensively, they failed to achieve the desired objectives. Sanctions cannot be separated from the threat of military intervention but, if sanctions can be targeted to inflict an increased level of hardship upon a defiant nation, then the intensity of the political objective which is reasonably attainable through the enforcement of sanctions can also be raised. The techniques available to escalate the level of sanctions may lie in evolving information technologies and their critical ties to international business.

EVOLUTION OF GLOBAL INFORMATION SYSTEMS

"Access to the outside world that high technology provides is seen by many countries, for example developing countries in Africa and Eastern Europe, as a means to participate in the overall growth of the international marketplace."[11] The critical link between access to international networks and the international business community presents a new target for sanctions: A country's information and communications infrastructure and particularly those aspects of that infrastructure which link domestic networks to the burgeoning Global Information Infrastructure (GII) have become key facets of the economic lines of communications which sustain the emerging global economy. Businesses unable to access international networks will be greatly hampered in carrying out even routine day to day operations. Both domestic and international telecommunications service providers continue to evolve to keep pace with the rapidly advancing requirements for globally connected information services. The following paragraphs will trace the ongoing evolution of this global infrastructure and serve to highlight the growing reliance of domestic economies on these global networks.

The telecommunications networks of today have evolved from austere telegraph services which originated in the North America and Europe in the 1830's. As early as 1860, the requirement to link the national domestic networks of these two continents was fulfilled with the laying of telegraph cables across the English Channel and the Atlantic Ocean.[12] Transoceanic telephony capabilities were established on a rudimentary basis in

1927 through the high frequency radio phone. Domestic telephone services were expanded through the use of cables and microwave radio techniques however, the range restrictions of these systems due to analog voice signal attenuation over distance and terrestrial propagation restrictions prevented the establishment of robust transoceanic links until the 1950's. The invention of the transistor during this time frame enabled the development of powerful signal amplifiers which made possible the construction of transoceanic cables and provided a means of fully connecting continental telephony networks.[13]

The transistor also served to usher in the digital age and the associated advents in telecommunications and computing. The transmission of digitized signals instead of analog signals enabled the development of digital filters, error correction coding, and compression techniques which extended the range over which signals could be transmitted as well as enhancing the quality of end to end services. The demand to link distant networks continues to expand and a growing array of satellites and fiber optic cables are being developed and installed to fulfill these requirements. The three facets that form this global network are the subscriber access terminal, domestic networks, and the telecommunications systems and associated standards which allow them to interface.

The ability of users or subscribers to employ instruments to access information networks has grown dramatically and has driven the explosion in associated network access and telecommunications services. With the advent of the telephone, individual users were provided with an instrument that facilitated direct access to networks. The

development of the computer and the ability to link computer networks has levied a new requirement for access to telecommunications services. Today, the prospect of providing subscribers with video teleconferencing services is changing the orientation of networking services and driving the increase of capacity in the communications pipes which link networks. The following paragraphs will outline the evolution of telecommunications services and service providers as they strive to pace the enhancements in subscriber terminal instruments. The requirements for domestic and international services and their ties to economic development will be reinforced.

Domestic telecommunications networks developed in close alignment with the governments of the nations which they served. In order to provide affordable services to the domestic subscriber, the cost of long distance services was artificially inflated.[14] In the United States, American Telephone and Telegraph (AT&T) provided all national domestic services as a privately owned government monopoly.[15] In Central Europe, during the 19th Century, the postal, telegraph, and telephone (PTT) systems were viewed as public services and placed under state administration.[16] In third world countries, domestic telecommunications systems originally owned and installed by private corporations were purchased by the state and subject to regulation similar to that of the European networks.[17] The telecommunications industry became "one of the most protected, insulated, and monopolized in the economies of virtually all nations."[18]

As the demand for domestic telephone services expanded, requirements for long haul communications paths to link national systems also expanded beyond the

capabilities of existing international cable systems. "Spurred on by technological advances and Cold War pressures, the United States enacted the Communications Satellite Act of 1962 to establish a commercial communications satellite system that would serve the nations of the world."[19] The act established the Communications Satellite Corporation (COMSAT) as a private, commercial organization which would be regulated by the United States government. COMSAT would plan and implement the commercial satellite system described in the 1962 act. COMSAT as the U.S. sole representative in this venture coordinated with the designated representatives of other countries and in 1964, an interim agreement was signed to establish the International Telecommunications Satellite Organization (INTELSAT). INTELSAT is an organization which consists of 139 member countries and currently operates 24 active INTELSAT communications satellites.[20] "Each member government appoints a signatory, usually a telecommunications agency or company with governmental ownership; the signatories are the investors in and the agents for the satellite system."[21]

As telecommunications systems evolved so did the governing organizations associated with them. In 1865, the International Telegraph Union was established in Paris, France.[22]As telephony and radio technologies emerged, the role of the organization was expanded. In 1932, the organization was renamed as the International Telecommunications Union (ITU) and in 1947, the ITU was made a specialized agency of the United Nations Administrative Council and chartered to provide telecommunications policy and direction. ITU specific duties include coordinating

frequency usage among nations, setting international telecommunications connectivity standards, coordinating allocation of satellite orbital slots, and setting tariffs for connection services.[23]

The ITU rules recognized the preeminence of these government appointed service providers. The development of the close linkage among telecommunications service providers, the governments which sanctioned them, and the body designated to regulate these agencies led to the development of a stable, monolithic telecommunications regime which was unhampered by the threat of competition. The norms under which this regime operated are outlined below.

> The implicit norms concerning the jurisdictional status of the airwaves and outer space have promoted the principals of the free movement of commerce and information while giving states the ultimate right to curtail foreign transmissions when they threaten domestic order. The norms with regard to damage control encourage the free flow of goods and services and the efficient use of the spectrum while offering a measure of equity for all countries.
>
> The major change in the telecommunications regime has occurred with regard to the sector of prices and market shares. From support for an intergovernmental cartel that promoted both efficiency and states' ability to control their domestic telecommunications systems, states have moved gradually since 1980 toward support of greater competition that reduces the costs of communications...[24]

The introduction of the competitive process into the telecommunications services arena, as described above, was initiated in the United States. In December, 1959, the Federal Communications Commission (FCC) allowed the creation of microwave networks which were independent from AT&T. In the 1960's the U.S. and other national monopolies began to lease portions of their telecommunications channels directly to

government and business firms (ITU rules specifically prohibited the sublease of circuits in order to ensure that services were provided solely by sanctioned governmental agencies). In the 1970's, the FCC ruled that firms other than AT&T were authorized to establish alternative networks; and in the early 1980's, the U.S. allowed additional entrants into the telecommunications market.[25]

These unilateral actions initiated within the U.S. would end in the break up of the AT&T monopoly. Japan and Britain followed the U.S. example. In the late 80's and early 90's the European Community, Canada, Australia, and New Zealand, liberalized the rules governing provision of telecommunications services and set the stage for open competition within their telecommunications markets.[26] "Movement toward competitive provision of basic telecommunications services and network infrastructure is gradually, stubbornly building momentum."[27]

The evolution to the telecommunications industry within the United States was highlighted in previous paragraphs. France and Sweden are examples of two other industrialized nations which are moving toward allowing competition within their domestic markets. In the case of France, French Telecom, which is the fourth largest telecommunications carrier in the world, was transformed to a private corporation on January 1, 1997.[28] The French decision to privatize their telecommunications industry was not only oriented toward lowering the cost of services but also aimed at posturing their domestic industry to compete in ".... an era where the telecommunications industry is expected to become a more important economic force than the automobile industry."[29]

Third world nations in particular are struggling with the drive toward privatization of telecommunications services but "the die is probably cast."[30]These nations lack the robust telecommunications infrastructures of developed nations and their associated state sanctioned telecommunications industry. For them, the prospect of privatization carries a fear that "... they would be dominated by a foreign/multinational entity that effectively would buy their entire telecommunications infrastructure. Instead of encouraging competition, this would merely replace a government-owned monopoly with superior technology under the aegis of foreign domination."[31]These nations also face the challenge of establishing a telecommunications infrastructure without subsidizing this foundation with excess profits from artificially inflated international services. A viable option for these nations may be a technology leap which avoids the installation of wire infrastructures and moves directly to the provision of service via a cellular infrastructure.[32]

The dismantling of the international telecommunications cartel can be attributed directly to the increasing requirements of the international business community, and a drive to gain enhanced services at a lower cost. The increased requirement for international communications links to support economic activity manifested itself through expansion of both fiber optic cable and satellite paths. The first transatlantic fiber optic cable was installed in 1988, and carried forty thousand channels. By 1995, four more cables had been installed each with increasing capacity up to one hundred and twenty thousand channels per cable.[33] The increase in international connectivity

requirements was not limited to transatlantic cables. In 1988, fiber optic cables provided services to 37 countries. By 1996, fiber optic cable services had been extended to nearly 100 countries.[34] The increased demand for international connectivity was also reflected among satellite providers. The capacity of INTELSAT constellation satellites expanded from with 240 channels supported by INTELSAT I in 1962, to the 120,000 channels supported by INTELSAT IV in 1990. As the number of satellites within the INTELSAT constellation grew, new competition within the industry spawned the creation of competing satellite communications service providers.

The growth in international communications capacity resulted in a decrease in the cost of doing international business. The cost of completing an international call in 1970 was three dollars per minute. Today, that same call will cost pennies per minute. The cost of leasing transoceanic cable circuits has been reduced by one fifteenth, and the cost of leasing satellite circuits has dropped by one eighth over this same time frame.[35] Nations which seek to compete within emerging international markets are finding that in order to attract business investment, they must offer telecommunications services at competitive rates.[36]

The move to privatization and competition within the telecommunications service arena has had the effect of forcing a monolithic cartel to evolve into the fastest growing industry in the world.[37] "The restructuring currently underway has given the industry an international dimension that is incompatible with national standardization and approval practices."[38] The capacity of the ITU to govern this fast growing and diverse industry is

also being challenged. The World Trade Organization has assumed an increasingly important role particularly in the adoption of commercial standards to ensure seamless telecommunications services.[39]

The growth of international telecommunications services correlates to the evolution of international business organizations. These organizations have generated information requirements which transcend borders and demand freedom of navigation through a growing global network. In order to provide the services required by international industry, telecommunications providers have also evolved from domestically controlled service providers to privately owned competitive businesses.

The increasing reliance of international businesses and by extension, the domestic economy of a country, upon international telecommunications systems lends credence to the hypothesis that strategic level information sanctions could be an effective tool, when linked with traditional forms of economic sanctions, in deterring conflict. Conversely, the evolution of telecommunications service providers into diverse, internationally owned, competitive businesses makes the process of enforcing information sanctions against a target country much more dependent upon achieving international support for the sanctions. This analysis is supported by the background case studies of the implementation of conventional sanctions which emphasizes that sanctions enforcement cannot be effectively accomplished without comprehensive action by the United Nations.

ENFORCEMENT OF INFORMATION SANCTIONS

As outlined previously, recent military operations involving enforcement of sanctions have not been oriented toward the interdiction of information, however, military operations against a nation's strategic information links are not without historical precedent. "At the outset of World War I, for example, the Royal Navy retrieved from the ocean floor and cut all the submarine telephone cables that linked Germany to the rest of the world, thus preventing independent [wired] communications between Germany and the neutral nations."[40] In spite of this example, actions to interdict a nation's access to strategic level networks are not prevalent. Military interdiction operations have been oriented toward the enemy armed forces' command and control (C2) systems after the commencement of hostilities. Offensive operations of this type have been defined as C2 warfare (C2W) operations.

The Air Force and Army have lead the development of information warfare doctrine within the Department of Defense (DOD). "The initial draft of the Air Force's effort to develop doctrine for IW addresses the issue of strategic attack in the information 'realm'... and makes fractionalizing the coherence of national centers of power as the basic objective of such attacks. Facilities such as microwave or telecommunications facilities (both of which were key target categories attacked during the Gulf War Air Campaign) are cited as examples of critical national information systems."[41] Although the services are working to refine IW, or as the Army refers to as

Information Operations (IO), these efforts have focused toward traditional roles of attack against enemy military C2 nodes and have not addressed IO as a strategic level operation which requires interagency coordination.[42]

The concept of implementing and enforcing information sanctions raises information operations above this definition to the strategic level of deterrent operations. Strategic level information operations imply that the nation initiating these operations possesses:

> .... sufficient information about an adversary's national-level political, economic, military and social systems to successfully operate against those systems and accomplish strategic political and military objectives; the means used may include diplomatic and economic actions, as well as destructive or non-lethal military operations... it will also include possessing knowledge and comprehension (i.e. 'situational awareness') of strategic centers-of-gravity such as the critical nodes in the enemy's national infrastructure; how their political and other vital systems function; whether these systems possess exploitable vulnerabilities; how their informational and financial networks function, etc.[43]

The preceding paragraph concisely describes the expertise that would be required to effectively target and enforce information sanctions. The required expertise to identify and attack information targets of this nature falls beyond the realm of strictly military targeting and clearly requires interagency participation. The agency tasked with the mission of enforcing information sanctions during the deterrent phase of a developing crisis must remain closely tied to the agencies which will execute the information warfare campaign once conflict begins. This close coordination is needed in order to ensure the orderly transition from deterrent operations to C2W operations should conflict ensue.

Efforts within the United States to address strategic level information operations

have been focused on protecting our growing information infrastructure. These defensive efforts have evolved as a result of the realization that the nation is increasingly dependent upon its information infrastructure. "The electronic web of computers and information technology touches virtually every element of U.S. domestic infrastructures. Besides telecommunications, the nation's financial systems, stock and commodity exchanges, air traffic control systems, electric power and distribution systems, and transportation networks all increasingly depend on IT [information technology] networks for their operation and health."[44]The expertise required to protect the vital and vulnerable United States information infrastructure is complimentary to the mission of wrecking an adversaries information infrastructure. The U.S. policy toward the employment of information sanctions has not been articulated, and the responsibility for the protection of the national public network against hostile information operations has been distributed among several federal agencies. The following paragraphs will trace national efforts to defend the growing national information infrastructure and provide insight into the complementary aspect of denying infrastructure services to a targeted nation.

The criticality of our national public network and its associated vulnerabilities was first highlighted as a result of a Cuban Missile Crisis. Difficulties in obtaining reliable communications during this crisis highlighted the need for a reliable communications infrastructure and led President Kennedy to formally establish the National Communications System (NCS) in 1963.[45] The role of providing reliable national services initially fell to AT&T, but with the divestiture actions of 1984, the

government could no longer rely upon a single source provider to coordinate infrastructure services. Recognizing the requirement for a joint government-industry team, the President's National Security Telecommunications Advisory Committee (NSTAC) was established. The NSTAC consisted of 30 members of the nation's largest telecommunications and information technology companies and was tasked with advising the President on telecommunications policy and issues.[46]

The NSTAC provided a government/industry team which could oversee the myriad elements of the nation's growing public networks and had the authority to act quickly to restore public network services during time of crisis.[47] The focus of the NSTAC has shifted from networks which were telephony based to the multimedia networks of today (voice, data, and video). The increasing vulnerability of today's computer based networks has been identified through recent studies. Recent reports from both the NSTAC and the Defense Science Board (DSB), cite numerous information infrastructure vulnerabilities as well as vulnerabilities in control systems which link the information infrastructure to other more traditional critical infrastructures. The report concluded that the nation's political, military, and economic interests are at risk.[48]

The increasing vulnerability of public, private, and government networks has received growing attention from the organizations owning these networks and resulted in the creation of organizations focused upon assuring information integrity within specified segments of the national information infrastructure. From a public network perspective, the National Coordinating Center (NCC) monitors the status of public networks for the

NSTAC. Within the DOD arena, the Global Operations Security Center (GOSC) has been established in order to monitor the status of information networks owned by the Defense Information Systems Agency (DISA).[49] This piecemeal approach to network security begins to break down as networks become more closely intertwined and integrated. As an example of this interdependence, DOD has become increasingly dependent upon access to the national information infrastructure. It is estimated that 95 percent of DOD traffic travels outside of DISA owned infrastructure at some point.[50]

The DSB report asserts that the existence of multiple organizations striving to assure information integrity with no coherent focus will not provide information assurance across the vast national information infrastructure. Even within the Federal government, the responsibilities for information warfare overlap multiple agencies. The report recommends that the Assistant Secretary of Defense (ASD) for Command, Control, Communications, and Intelligence (C3I) be charged with the mission of "piloting this new wing of warfare."[51]ASD C3I would assume responsibility for defending the federal infrastructure as well as conducting offensive information operations. A related National Research Council report recommends the establishment of a proposed organization to be called the Information Systems Security Board (ISSB). The ISSB would be an NSTAC entity whose tasks would include promoting the use of information security methods, systems, and products.[52]

The common thread that runs through various reports related to the vulnerabilities of the United States information infrastructure is that there is no single entity in charge of

even the defense of our domestic national infrastructure. The acceptance of the DSB recommendation to assign the ASD C3I this responsibility as well as the responsibility for strategic level offensive IW operations would focus the efforts of several federal agencies. The close coordination of the ASD C3I with the ISSB (advocate for commercial security practices) is required in order to ensure the veracity of domestic infrastructure protection techniques and provide the ASD C3I executive agent with the technical skills required to carry out strategic information operations to include the enforcement of information sanctions.

CONCLUSIONS

The process of implementing strategic information sanctions during the deterrent phase of an evolving crisis in order to achieve our national objectives has not been fully explored. Within the U.S., activities related to the implementation of information sanctions have focused upon protection of the national information infrastructure and offensive C2W operations which target a nation's domestic infrastructure after hostilities commence. The explosive growth of information technologies and their correlation with the economic well being of the nation that they serve provides a potentially persuasive tool for crisis resolution short of conflict. Information sanctions operations must take into consideration the shift in character which has taken place among providers of telecommunications services, and indentify the interagency process through which information sanctions can be effectively implemented.

The shift in character of domestic telecommunications service providers from sovereign ownership with an intranational connectivity focus, toward private ownership with an international focus has served to create an environment in which the enforcement of information sanctions is not straightforward. The privatization of a business which was once nationally controlled and regulated has spawned a diverse and growing group of competitive companies. These privately owned commercial telecommunications firms compete for business within a growing international market and provide services which transcend national borders. The increase in the number of telecommunications service

providers, the multinational nature of these companies, and the increased accessibility of the global information infrastructure combine to make the task of enforcing information sanctions complex. The fact that telecommunications companies within the United States are the world's largest exporters of these technologies portends situations which present a conflict between the national security and economic interests of our country.

The evolving international character of telecommunications businesses and their legal obligations to provide services to their clients will present an environment in which unilateral sanctions may not be enforceable. In order to deprive a customer of contracted service, the business must be ordered to do so by competent legal authority and the targeted nation must be prevented from contracting information services from another competitor. In order to be enforceable, information sanctions will have to be backed by United Nations resolutions and closely coordinated with the World Trade Organization (WTO).

Although the growing multinational composition and competitiveness of international telecommunications service providers serves to make the process of information sanctions enforcement more complex, the explosion in the growth of international connectivity requirements reflects the growing importance of information as an international business commodity. The role of information systems within the international market place will continue to grow as the functionality of subscriber terminals continues to expand. As information technologies evolve to support single subscriber terminals which provide private voice, data, and teleconferencing services, the

reliance on these systems to conduct expanding aspects of day to day business will also increase. International finance, marketing, and planning will be conducted electronically and these activities will become facilitators of, and in some case precursors for, the physical exchange of goods and products. Comprehensive economic or other specified sanctions will carry with them information components which must be included as part of sanctions enforcement mandate if the sanctions are to be effective.

Sanctions enforcement operations will be expanded from the physical interdiction of ships, ground vehicles, and aircraft, to the interdiction of telecommunications lines of communication and information carrying 'vessels' which connect the target nation's domestic information infrastructure to the global information network. The enforcement of these sanctions will require forces which have insight into the target nation's information infrastructure and have the assets and expertise to monitor the flow of information in and out of the target country. The target of information sanctions will be predominately commercial systems which provide subscriber services to multiple nations. Denial of access to the target nation without disrupting services to other clients will require close coordination with the commercial entity controlling that system and eliminate physical destruction of the system as a course of action. The composition of the forces which monitor the enforcement of information sanctions must include international telecommunications industry representation.

Unlike destructive C2W operations which will be undertaken in the event of conflict, information sanctions must focus on denial of international access by gleaning

international support. Sanctions must include a process through which corporations impacted by sanctions implementation will be compensated and specify secondary sanctions which will be imposed upon corporations which violate the primary sanctions. The key to successful sanctions enforcement will be the ability to monitor the information lines of communications which link the target nation to the international community and the identification of entities which provide international information services in defiance of UN/WTO resolutions.

The form of information sanctions imposed must be tailored based upon the information system and telecommunications architecture of the nation which is the target of the sanctions. Sanctions should focus upon the international telecommunications links which provide the national infrastructure access to international networks. The more robust and diverse the national architecture, the more difficult it will be to fully cut access to international systems. Full disruption of all international communications links may not be desirable as diplomatic initiatives and information campaigns may rely upon access to the target nation leadership and general population respectively. The process of identifying key telecommunications links (channels on a commercial satellite or channels over a commercial cable) and selectively depriving the target nation of access to those paths would aim at restricting access to international networks and compliment other related sanctions (economic or specified goods).

The implementation of information sanctions in conjunction with traditional forms of sanctions will enhance the power within this diplomatic tool. The threat of

enforcing a comprehensive sanctions package which includes restriction of access to international information sources will present target nations with a situation in which their domestic economy will be severed from the sustaining resources of the international economy.

The threat of implementing information sanctions must be backed with the wherewithal to enforce the sanctions once imposed. Should the U.S. recognize the potential utility of information sanctions in deterring conflict, then Department of State (DOS) efforts to secure comprehensive UN/WTO sanctions resolutions must include the commodity of information. Subsequent sanctions enforcement operations by military forces must be limited to monitoring effectiveness of information sanctions and identifying those nations or corporations which provide sanctioned services. The ASD C3I must designate the lead agent to monitor sanctions effectiveness. This unit or task force must closely coordinate with UN/DOS representatives to identify sanctions violators and with UN/DOD follow on forces designated to conduct offensive operations should deterrent measures fail. As with traditional sanctions, even comprehensively orchestrated and enforced sanctions may not force a recalcitrant nation to alter its course of action once committed. However, the threat of such comprehensive sanctions, if conveyed prior to conflict, could serve to enhance the power and effectiveness of deterrent operations.

ENDNOTES

[1]National Military Strategy of the United States of America. (Washington: U.S. Government Printing Office, 1995) 12.

[2] Daniel T. Kuehl, "Strategic Information Warfare and Comprehensive Situational Awareness," in Cyberwar: Security, Strategy and Conflict in the Information Age. ed. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, 185-196, (Fairfax, VA: AFCEA International Press, 1996). 186.

[3] Ibid.

[4]Arnold Kantner and Linton F. Brooks, U. S. Intervention Policy for the Post-Cold War World. (New York: W.W. Norton & Company Inc, 1994) 63.

[5]Ibid.

[6]Ibid., 147.

[7]Ibid., 148.

[8]Ibid.

[9]Ibid., 149.

[10]Ibid., 157.

[11]Ibid., 163.

[12]Mark W. Zacher with Brent A. Sutton, Governing Global Networks: International Regimes for Transportation and Communications. (Great Britain: Cambridge University Press, 1996) 127

[13]Ibid., 128.

[14]Report to the Chairman, Committee on Commerce, Science and Transportation, U.S. Senate, TELECOMMUNICATIONS: Competition Issues in International Satellite Communications. (Washington: U.S. Government Accounting Office, October, 1996) 17.

[15]Zacher and Sutton, 163.

[16]Ibid., 162.

[17]Ibid.

[18]Ibid.

[19]TELECOMMUNICATIONS: Competition Issues , 20.

[20]Ibid, 21.

[21]Ibid.

[22]Zacher and Sutton, 132.

[23]Ibid., 134.

[24]Ibid.

[25]Ibid., 167.

[26]Ibid., 169.

[27]Ibid., 172.

[28]D.J. Suberk and Robert K. Ackerman, "France Banks on Privatization to Boost Telecommunications." SIGNAL, December, 1996, 35.

[29]Ibid.

[30]Zacher and Sutton,173.

[31] "Emerging Nations Ponder Infrastructure Challenges."SIGNAL, December, 1996, 34.

[32]Ibid.

[33]Zacher and Sutton, 129.

[34]TELECOMMUNICATIONS: Competition Issues , 37.

[35]Zacher and Sutton, 130.

[36]Ibid., 169.

[37]Ibid., 130.

[38]Ibid., 160.

[39]Ibid., 173.

[40]Kuehl, 190.

[41]Ibid., 189.

[42]Ibid.

[43]Ibid., 185.

[44]James Kerr, "Information Assurance: Implications to National Security and Emergency Preparedness" in Cyberwar: Security, Strategy and Conflict in the Information Age. ed. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, 257-266 (Fairfax, VA: AFCEA International Press, 1996). 263.

[45]Ibid., 257.

[46]Ibid., 258.

[47]Ibid.

[48]"Industry, Government Pursue Data Security Clearinghouse," SIGNAL, March, 1997, 69.

[49]Ibid.

[50]Martin C. Libicki, "Protecting the United States in Cyberspace." in Cyberwar: Security, Strategy and Conflict in the Information Age. ed. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, 91-106. (Fairfax, VA: AFCEA International Press, 1996. 92.

[51]"Industry, Government Pursue...", 70.

[52]Ibid., 71.

BIBLIOGRAPHY

[1]Kerr, James. "Information Assurance: Implications to National Security and Emergency Preparedness." in Cyberwar: Security, Strategy and Conflict in the Information Age. ed. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, 13-30. Fairfax, VA: AFCEA International Press, 1996.

[2]Kantner, Arnold and Brooks, Linton F. U. S. Intervention Policy for the Post- Cold War World. New York: W. W. Norton & Company Inc. 1994.

[3]Kuehl, Daniel T. "Strategic Information Warfare and Comprehensive Situational Awareness." in Cyberwar: Security, Strategy and Conflict in the Information Age. ed. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, 13-30. Fairfax, VA: AFCEA International Press, 1996.

[4]Libicki, Martin C. "Protecting the United States in Cyberspace." in Cyberwar: Security, Strategy and Conflict in the Information Age. ed. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, 13-30. Fairfax, VA: AFCEA International Press, 1996.

[5]Suberk, D. J. and Ackerman, Robert K. "France Banks on Privatization to Boost Telecommunications." SIGNAL, December 1996, 33-36.

[6]Zacher, Mark W. with Sutton, Brent A. Governing Global Networks: International Regimes for Transportation and Communications. Great Britain: Cambridge University Press, 1996.

[7]"Emerging Nations Ponder Infrastructure Challenges." SIGNAL, December, 1996, 34.

[8]"Industry, Government Pursue Data Security Clearinghouse." SIGNAL, March, 1997, 69-71.

[9] National Military Strategy of the United States of America. Washington: U. S. Government Printing Office, 1995.

[10]Report to the Chairman, Committee on Commerce, Science and Transportation, U. S. Senate. TELECOMMUNICATIONS: Competition Issues in International Satellite Communications. Washington: U. S. Government Accounting Office, October, 1996.